PATENT COOPERATION TREATY

From the INTERNATIONAL BUREAU

# PCT

**NOTIFICATION OF ELECTION**

(PCT Rule 61.2)

To:

Assistant Commissioner for Patents
United States Patent and Trademark Office
Box PCT
Washington, D.C.20231
ETATS-UNIS D'AMERIQUE

in its capacity as elected Office

| | |
|---|---|
| **Date of mailing** (day/month/year)<br>28 September 2000 (28.09.00) | |
| **International application No.**<br>PCT/US00/02101 | **Applicant's or agent's file reference**<br>18926-38PC |
| **International filing date** (day/month/year)<br>28 January 2000 (28.01.00) | **Priority date** (day/month/year)<br>29 January 1999 (29.01.99) |
| **Applicant**<br>MORONEY, Paul | |

1. The designated Office is hereby notified of its election made:

[X] in the demand filed with the International Preliminary Examining Authority on:

25 August 2000 (25.08.00)

[ ] in a notice effecting later election filed with the International Bureau on:

2. The election [X] was
[ ] was not

made before the expiration of 19 months from the priority date or, where Rule 32 applies, within the time limit under Rule 32.2(b).

**The International Bureau of WIPO**
**34, chemin des Colombettes**
**1211 Geneva 20, Switzerland**

Facsimile No.: (41-22) 740.14.35

Authorized officer

F. Baechler

Telephone No.: (41-22) 338.83.38

5\11 52
09/890179

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

CORRECTED VERSION

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
3 August 2000 (03.08.2000)

PCT

(10) International Publication Number
WO 00/45273 A1

(51) International Patent Classification[7]: G06F 12/14

(21) International Application Number: PCT/US00/02101

(22) International Filing Date: 28 January 2000 (28.01.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/117,788 29 January 1999 (29.01.1999) US
60/128,772 9 April 1999 (09.04.1999) US

(71) Applicant (*for all designated States except US*): GENERAL INSTRUMENT CORPORATION [US/US]; 101 Tournament Drive, Horsham, PA 19044 (US).

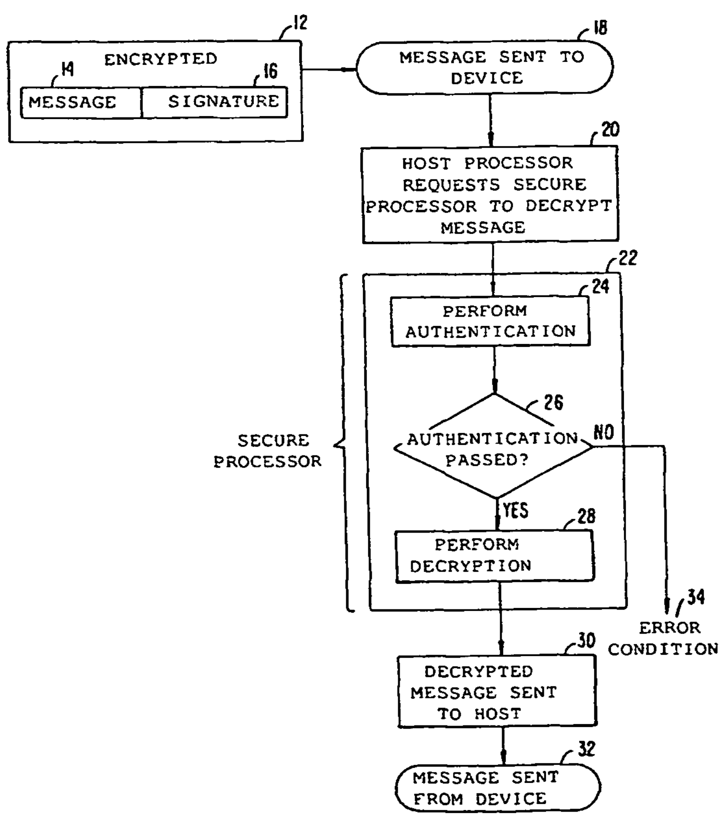
(72) Inventor; and
(75) Inventor/Applicant (*for US only*): MORONEY, Paul [US/US]; 3411 Western Springs Road, Olivenhain, CA 92124 (US).

(74) Agents: KULAS, Charles, J. et al.; Townsend and Townsend and Crew LLP, 8th Floor, Two Embarcadero Center, San Francisco, CA 94111 (US).

(81) Designated States (*national*): AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

*[Continued on next page]*

(54) Title: AUTHENTICATION ENFORCEMENT USING DECRYPTION AND AUTHENTICATION IN A SINGLE TRANSACTION IN A SECURE MICROPROCESSOR




(57) Abstract: The present invention uses a secure processor (22) operating with a host processor (210) to perform a unitary decrypt/authenticate operation. The host processor (210) receives encrypted messages (12) that include authentication information. The host processor must submit each message (12) to the secure processor (22). The secure processor (22) then decrypts and authenticates the message. If the authentication operation (24) is not successful, the secure processor (22) does not return the fully-decrypted message back to the host (210). In a preferred embodiment, the host (210) will receive no part of the message upon failure.

WO 00/45273 A1

(84) **Designated States** *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

**Published:**
— *with international search report*

(48) **Date of publication of this corrected version:**
21 February 2002

(15) **Information about Correction:**
see PCT Gazette No. 08/2002 of 21 February 2002, Section II

*For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.*

# AUTHENTICATION ENFORCEMENT USING DECRYPTION AND AUTHENTICATION IN A SINGLE TRANSACTION IN A SECURE MICROPROCESSOR

## CROSS-REFERENCES TO RELATED APPLICATIONS

This application claims priority from U.S. Provisional Patent Application Serial No. 60/117,788 filed on January 29, 1999 and from U.S. Provisional Patent Application Serial No. 60/128,772 filed on April 9, 1999, the disclosures of which are incorporated in their entirety herein by reference for all purposes.

## BACKGROUND OF THE INVENTION

This invention relates in general to secure data processing in digital systems and more specifically to a device that performs decryption and authentication using a secure processor.

Public key systems have become a very popular means for providing security in digital systems. Public Key Systems (PKS) have two different keys, one for encryption, or signing, and one for decryption, or verifying. This separation of keys has great security value in that the sign/decrypt function can be securely isolated from verify/encrypt functions, as is appropriate for the typical use of these keys. Public key systems are also known as asymmetric systems, or cryptosystems, as opposed to non-public key systems that are known as symmetric, or secret key, systems.

To send a message in a public key system, a sender obtains the receiver's public key. The sender uses the public key to encrypt a message. The encrypted message is then sent to the receiver. Since only the receiver has the corresponding private key of the

public/private key pair, only the intended receiver can decrypt and view the encrypted message.

However, a problem arises in that the sender may not be sure that they have obtained the receiver's correct public key in the first place. For example, a fraudulent public key may have been provided under the guise of the receiver's public key. In order to prevent this, "certificates" are used to generate confidence in the legitimacy of a public key. A certificate is typically the information that is included along with a signed message, where the certificate includes the public key required to verify the signature on the message. The certificate is signed with the certifying authority's private key and can be verified by a recipient of the certificate by using the certifying authority's public key. Of course, the same problem of obtaining the known certifying authority's correct public key in the first place still exists. A sequence of certified public keys can be obtained from sources of progressively higher trust, where each preceding certificate's public key comes from a successively more trustworthy source. At some point, the user of a certificate's public key must be able to trust, or be assured that, the original public key for the chain of certificates does, indeed, come from the proper source and is valid.

The act of user authentication (verification of user identity) usually includes the verification of the user's certificate. Usually the certificate includes the identity of the sender, the identity of the certificate issuer, the sender's public key, the time period for which the certificate is valid, etc.

Sometimes it is necessary to update key pairs by sending new key pairs from one device to another. This procedure can benefit from being validated by certificates, but where the updating occurs frequently the inclusion of certificate processing can put a high processing burden on the participating systems. Also, certificates need to be generated, signed and transferred in order to minimize the effect that a "broken" or "stolen" private key could have on a system. The maintenance of security based on a public key scheme, certificates, authentication, etc., is referred to as a system's Public Key Infrastructure (PKI). An example of telecommunications systems where the implementation of a traditional PKI is problematic or prohibitive is in a large scale digital network, such as the Internet. Where the data being transferred is high bandwidth using many transactions of small size, the number of

discrete exchanges of data, along with their corresponding encryption, decryption, authentication, etc., is extremely large. However, the need for security such as is provided by a PKI is also great, especially in applications such as telephony, or other secure data transfers such as banking, etc.

Devices that process secure, or encrypted, information often use secure processors, or microprocessors, that are designed to prevent intrusion into, and unwanted tampering or misuse of, the processor. A problem with secure processors is that they must be tightly controlled by a manufacturer, or "owner," of the processor, or device within which the processor resides. Thus, it is difficult to provide an "open architecture" for third party developers, customers, etc., of the devices. One way to alleviate this problem is to include both a secure processor and an "unsecure processor" (or, simply, "processor"). The unsecure processor has lowered security that allows third party developers to have relatively free access to the processor and the processor's resources such as memory, support chips, etc., so that the third party can develop and install software to upgrade or change the device's functionality. Typically, the unsecure processor attends to systems and control functions and makes calls to, or requests of, the secure processor to decrypt messages, authenticate information and perform other security functions. In this role, the unsecure processor is also referred to as a "host" processor.

However, a problem with the host processor/secure processor approach is that it can reduce the overall security of the device. This is because the host processor has control over which messages, or other information, are submitted to the secure processor for decryption. Since the host processor can easily be reprogrammed, or otherwise controlled or "hacked" to perform security breaches, care must be taken that such breaches do not occur.

For example, in applications where a secure processor is called upon to perform authentication and decryption operations, the host processor is in a role of sending, or not sending, the information to the secure processor. Where the host processor makes requests of the secure processor for authentication, the host processor can be reprogrammed to "skip" the authentication operation, or to falsely state that the authentication operation was successful when, in fact, the authentication was not successful or never occurred.

Also, some systems use messages that are authenticated but not encrypted. This approach allows the host processor to have access to the contents of the unencrypted, "clear text," of the message whether or not the authentication is verified.

Thus, it is desirable to provide a device that overcomes one or more of the shortcomings of the prior art.

## SUMMARY OF THE INVENTION

The present invention uses a secure processor operating with a host processor to perform a unitary decrypt/authenticate operation. The host processor receives encrypted messages that include authentication information. The host processor must submit each message to the secure processor. The secure processor then decrypts and authenticates the message. If authentication is not successful, the secure processor does not return the fully-decrypted message back to the host. In a preferred embodiment, the host will receive no part of the message upon failure.

In one embodiment the invention provides a method for performing authentication of messages in a device, wherein the device receives encrypted messages, wherein the device includes a host processor coupled to a secure processor. The method includes receiving an encrypted message; using the secure processor to decrypt the message; using the secure processor to authenticate the message; and subsequent to the steps of using the secure processor, performing the step of determining whether the message is authentic and, if the message is authentic, then transferring the decrypted message to the host processor.

In another embodiment the invention provides a method of providing secure processing in a telecommunications sytem that transfers messages to devices, wherein one or more of the devices include a host processor and a secure processor and wherein a message has an associated authentication. The method includes encrypting the message and associated authentication.

## BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 is a flowchart showing basic steps of the present invention;

Fig. 2A shows a portion of a telephony network; and

Fig. 2B shows details of a cable telephony adapter.

## DESCRIPTION OF THE SPECIFIC EMBODIMENTS

The present invention is preferably included in a device referred to as a Cable Telephone adapter (CTA). The CTA is used in a cable telephony system that is described in detail in the priority documents referenced at the beginning of this specification. Although specific reference is made to a cable telephony system, the invention is adaptable for use in virtually any telecommunications system that uses secured transactions.

### Cable Telephony Adapter

FIG. 2A shows a portion of an IP telephony network 100 constructed in accordance with the present invention. The network 100 includes a first user 102 coupled to a source CTA 104. The source CTA 104 is further coupled to a source gateway controller 106 and an IP telephony network backbone 110.

The network 100 also includes a second user 112 coupled to a destination CTA 114. The destination CTA 114 is further coupled to a destination gateway controller 116 and the IP telephony network backbone 110. In addition, the network 100 also includes a customer service representative (CSR) center 120, a provisioning server 122 and a billing host 124.

Each user of the network 100 goes through an initialization process to activate network service. For example, when the user 102 and associated CTA 104 are coupled to the network, a series of messages are exchanged between the CTA 104, provisioning server 122, gateway controller 106 and the CSR 120. The messages provide for activation of telephony service for the user 102, establishment of account information and creation of encryption keys to be used by the CTA to encrypt and decrypt messages exchanged over the network. The billing host 124 is used to setup account information for each user and to bill for network

usage. The provisioning server 122 is used to initialize and register CTA devices within a specific IP telephony network.

Fig. 2B shows an exemplary embodiment of the CTA 104 constructed in accordance with the present invention. The CTA 104 includes a cable input interface (I/F) 202, a cable output I/F 204, a user output I/F 206, a user input I/F 208, a host processor 210, a memory 212 and an additional secure processor 220 along with secure memory 222, used to protect public/private key pairs 224. Certificates 214 are stored in regular memory because they are signed and don't require additional protection.

The cable input I/F 202 is coupled to a cable telephony input 216. The cable output I/F 204 is coupled to a cable telephony output 218. The cable telephony input and output I/F couple the CTA 200 to a cable telephony network, such as by connecting to a cable modem (not shown) that is coupled to the cable telephony network. In another embodiment, the cable modem is included in the CTA so that the cable telephony network may be connected directly to the CTA.

The processor 210 couples to the cable input I/F 202 and the cable output I/F 204 to provide processing of information received and transmitted, respectively, on the telephony network. The line 216 carries secure encrypted and/or signed information which cannot be processed directly by the host processor, since it does not have access to cryptographic keys. This includes provisioning information , call set-up and voice data. In cases where it is desired to perform secure authentication the host processor has to pass on this information to the secure processor, which has access to the necessary keys to perform cryptographic operations. The connections between the cable I/F modules and the user I/F modules carry unencrypted information. The unencrypted information is commonly referred to as clear text, which extends back to the user. Similarly, some clear text user input may need to be encrypted and/or signed securely. This cannot be done directly by the host processor. It passes on the information to the secure processor that performs the cryptographic operations. This way, encrypted and/or signed data appears on line 218.

The certificates in 214 cryptographically bind each public key to an identity. The short, self-signed public key may be bound to either the device or user identity, while the longer public keys installed at the time of manufacture must be bound to the identity of the

device (since the user identity is unknown at that time). The certificates are not protected in secure memory because they are already cryptographically protected with a digital signature.

**Combined Decryption/Authentication**

Fig. 1 is a flowchart that describes the basic steps of the present invention.

In Fig. 1, message 12 is received by a device such as the CTA of Figs. 2A and 2B. Message 12 includes message information 14 and signature 16.

Step 18 represents receipt of the message at the device. Transfer to, and receipt of, the message can be by any means. For example, the radio-frequency transmission, hardwire, fiber optic, acoustic, etc., channels can be used. Any suitable telecommunications network can be employed such as the Internet, cable television, satellite, telephone, etc. Any suitable protocols can be used. Receipt is performed by Cable Input Interface 202 of Fig. 2B. Upon receipt, the message is under the control of host processor 210. Other embodiments can use other means to receive the message. For example, the message can be provided directly to secure processor 220 without the need for host processor 210 to mediate.

Once received, step 20 is executed where the host processor transfers the message to the secure processor and requests decryption. Steps 24, 26 and 28 are performed by the secure processor and the secure processor's resources, as indicated by box 22.

At step 24, the secure processor performs authentication. In this case, signature 16 is verified by processing it with a public key. Other forms of authentication are possible. E.g, Symmetric key authentication, public key encryption, etc., are possible variations. At step 26 a check is made as to whether the authentication passed. If not, an error condition exists and the host processor will not receive the same information as when authentication passes. In the preferred embodiment, the host processor receives notification that the authentication failed. The host processor will receive no decrypted information in the message. Other embodiments may inform other devices in the system that an authentication has failed. Also, some of the encrypted information can still be decrypted and transferred to the host. This may be useful for service or troubleshooting as where a key has expired and the secure processor gives notice of the expiration date of a key, certificate, etc.

Assuming authentication passed, step 28 is executed by the secure processor to perform decryption on the message. Note that this embodiment uses an overall encryption on the message. Since decryption and verification keys are held only by the secure processor, and it supports only a single decryption and authentication operation, it is impossible to separate the two at the host processor level where the information is still encrypted. After decryption, the message information is sent to the host processor at step 30. Finally, the host processor can direct that some or all of the message information (or other information generated in response to the message information) be further processed.

Variations are possible from the arrangement shown in Fig. 1. For example, decryption can be performed before a check for authentication. In one form the signature could be encrypted and then must be decrypted before the authentication step can be performed. However, in another embodiment the message can be decrypted at the same time the signature is verified. If authentication then fails, the decrypted message can be discarded. This is not a security threat because the decrypted message is stored in secure memory 222. There may be speed advantages in such parallel processing.

Note that steps can be added to, or taken away from, the arrangement shown in Fig. 1. For example, step 20 of the host processor requesting the decryption can be omitted where the messages automatically are sent to the secure processor for decryption. Additional steps such as storing of the message, stripping of header information or data fields, etc., can be performed before, after, or during secure processing.

Thus, although the invention has been presented with respect to specific embodiments thereof, these embodiments are merely illustrative, and not restrictive, of the invention, the scope of which is to be determined solely by the appended claims.

WHAT IS CLAIMED IS:

1. A method for performing authentication of messages in a device, wherein the device receives encrypted messages, wherein the device includes a host processor coupled to a secure processor, the method comprising

receiving an encrypted message;

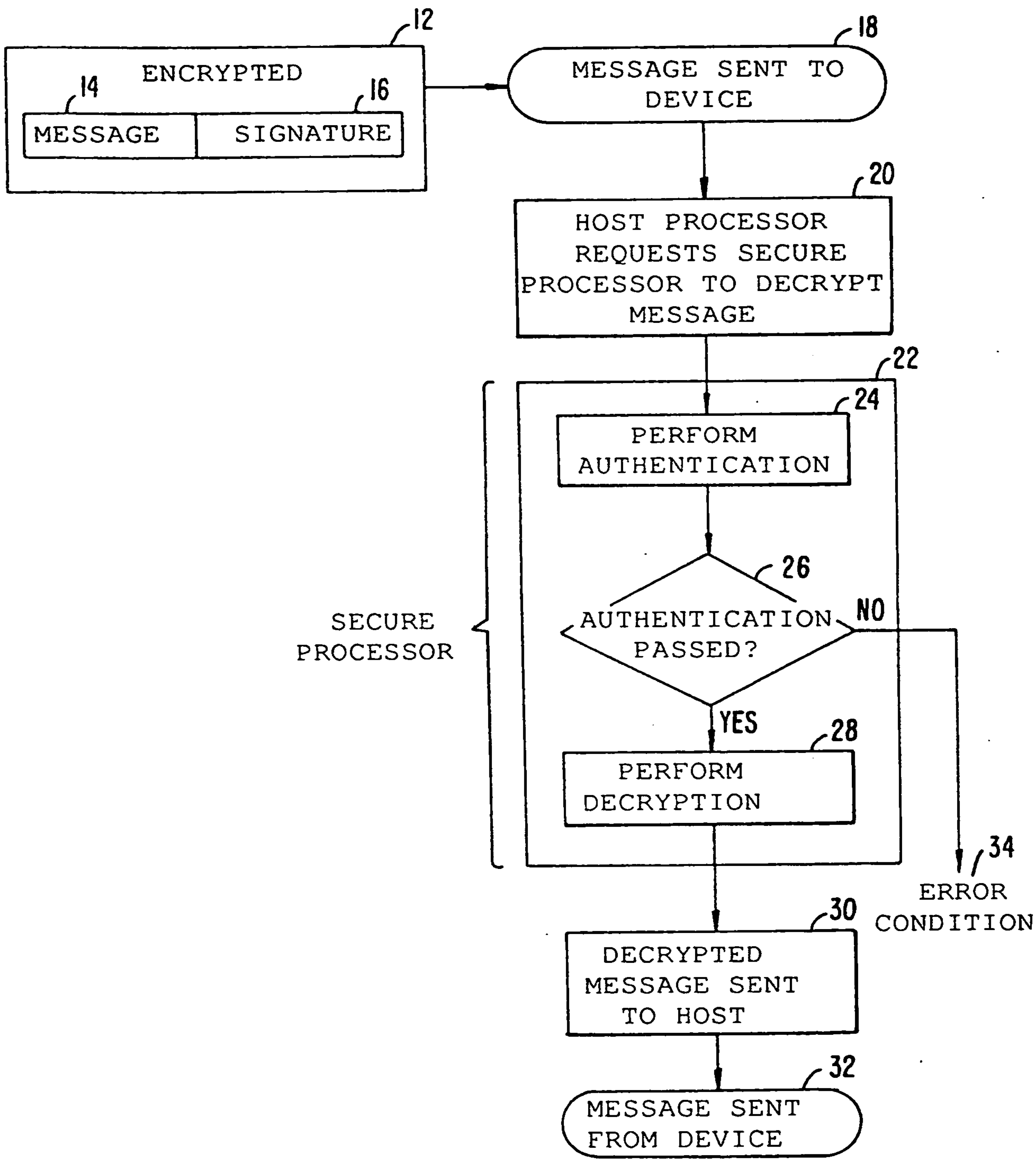
using the secure processor to decrypt the message;

using the secure processor to authenticate the message; and

subsequent to the steps of using the secure processor, performing the step of determining whether the message is authentic and, if the message is authentic, then transferring the decrypted message to the host processor.

2. A method of providing secure processing in a telecommunications sytem that transfers messages to devices, wherein one or more of the devices include a host processor and a secure processor, wherein a message has an associated authentication, the method comprising

encrypting the message and associated authentication.



12
ENCRYPTED
14
MESSAGE
16
SIGNATURE
18
MESSAGE SENT TO DEVICE
20
HOST PROCESSOR REQUESTS SECURE PROCESSOR TO DECRYPT MESSAGE
22
24
PERFORM AUTHENTICATION
26
AUTHENTICATION PASSED?
NO
YES
28
PERFORM DECRYPTION
SECURE PROCESSOR
34
ERROR CONDITION
30
DECRYPTED MESSAGE SENT TO HOST
32
MESSAGE SENT FROM DEVICE


FIG. 1.

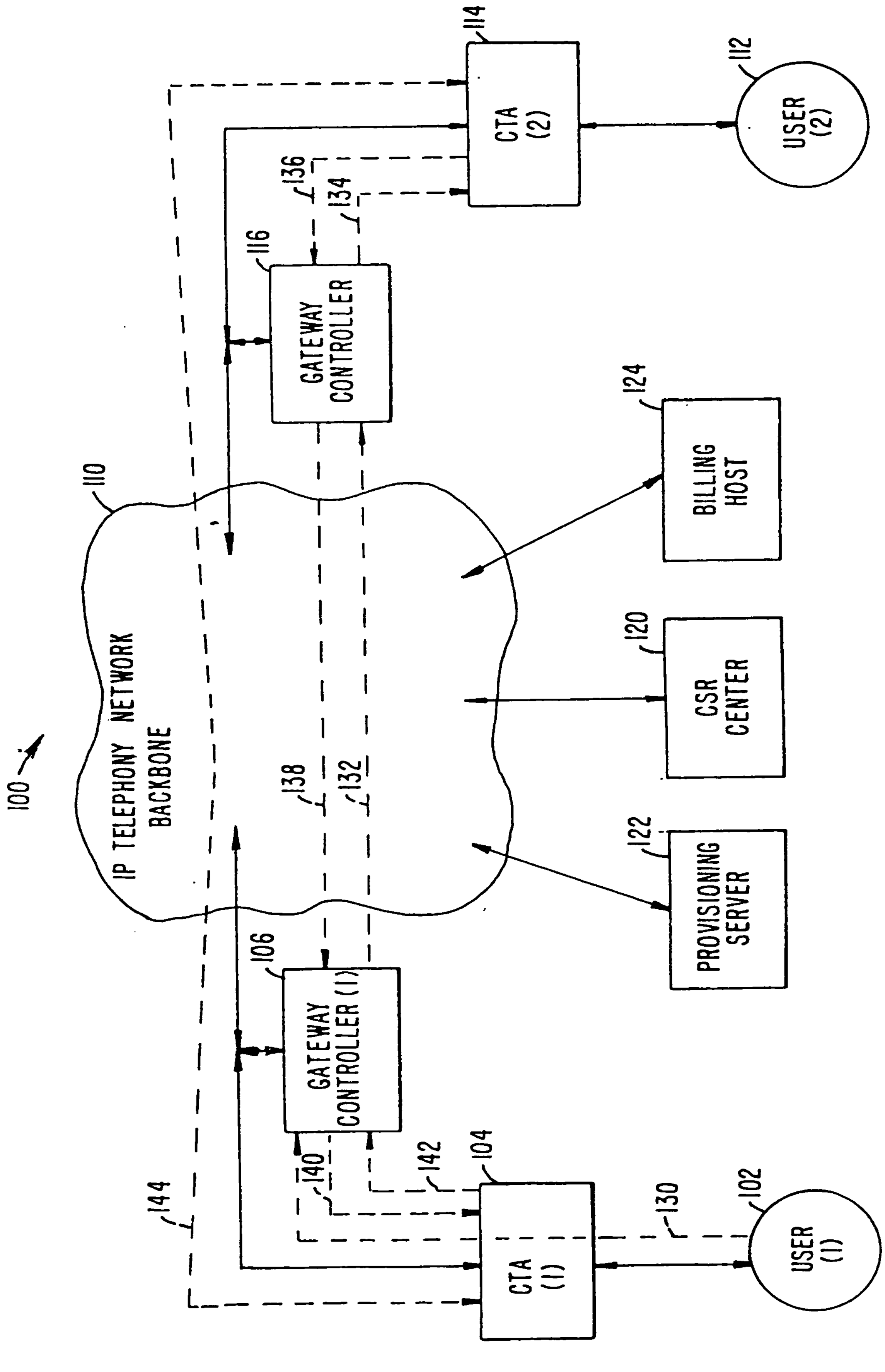

100
110
IP TELEPHONY NETWORK BACKBONE
114
CTA (2)
112
USER (2)
116
GATEWAY CONTROLLER
136
134
138
132
124
BILLING HOST
120
CSR CENTER
122
PROVISIONING SERVER
106
GATEWAY CONTROLLER (1)
140
142
144
104
CTA (1)
130
102
USER (1)

FIG. 2A.

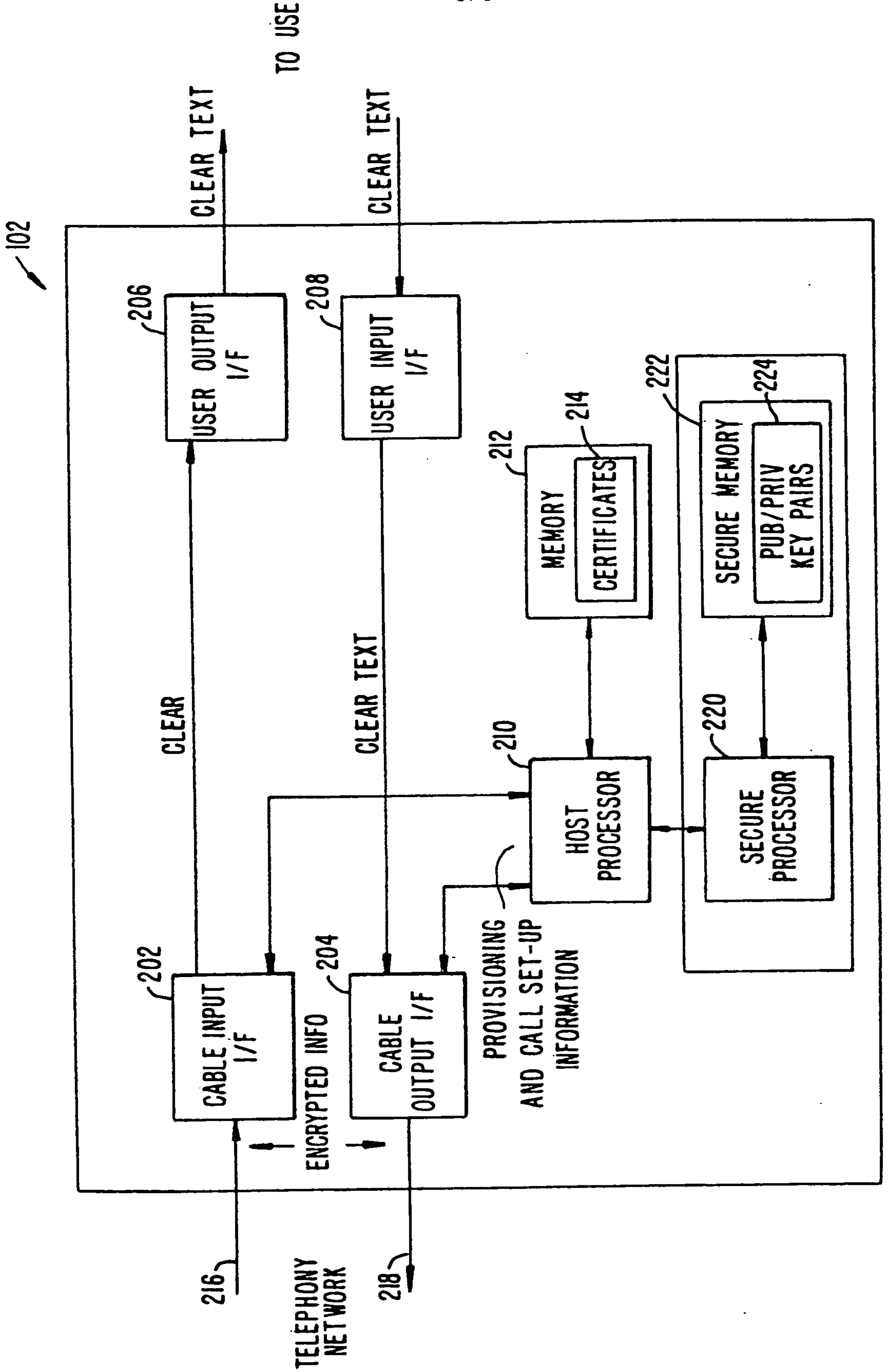

102
TO USER
CLEAR TEXT
CLEAR TEXT
206
USER OUTPUT I/F
208
USER INPUT I/F
CLEAR
CLEAR TEXT
212
MEMORY
214
CERTIFICATES
222
SECURE MEMORY
224
PUB/PRIV KEY PAIRS
210
HOST PROCESSOR
220
SECURE PROCESSOR
202
CABLE INPUT I/F
204
CABLE OUTPUT I/F
ENCRYPTED INFO
PROVISIONING AND CALL SET-UP INFORMATION
216
218
TELEPHONY NETWORK

FIG. 2B.

**INTERNATIONAL SEARCH REPORT**

| International application No. |
|---|
| PCT/US00/02101 |

**A. CLASSIFICATION OF SUBJECT MATTER**

IPC(7) : G06F 12/14

US CL : 713/155, 156, 168, 170, 171, 180, 200, 201, 202

According to International Patent Classification (IPC) or to both national classification and IPC

**B. FIELDS SEARCHED**

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 713/155, 156, 168, 170, 171, 180, 200, 201, 202

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

Please See Extra Sheet.

**C. DOCUMENTS CONSIDERED TO BE RELEVANT**

| Category* | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| X | US 5,838,792 A (GANESAN) 17 November 1998, col. 4, line 64-col. 17, line 16. | 1-2 |
| A | US 5,535,276 A (GANESAN) 09 July 1996, the whole document. | 1-2 |
| A,P | US 5,923,759 A (LEE) 13 July 1999, the whole document. | 1-2 |
| A,P | US 5,935,249 A (STERN et al) 10 August 1999, the whole document. | 1-2 |

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"B" earlier document published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

| Date of the actual completion of the international search | Date of mailing of the international search report |
|---|---|
| 17 MAY 2000 | 19 JUN 2000 |

| Name and mailing address of the ISA/US | Authorized officer |
|---|---|
| Commissioner of Patents and Trademarks<br>Box PCT<br>Washington, D.C. 20231 | Reba Elmore Joni Hill |
| Facsimile No. (703) 305-3230 | Telephone No. (703) 308-7098 |

## INTERNATIONAL SEARCH REPORT

International application No.
PCT/US00/02101

B. FIELDS SEARCHED
Electronic data bases consulted (Name of data base and where practicable terms used):

BRS/WEST, EAST
(authenticate or permit or authorize) ; (message or data or information); secure; (encrypt or signing); (decrypt or verifying)